Yahoo!

Build Brands Members Love

https://www.yahoo.com · @yahoo

Reports resolved	Assets in scope	Average bounty
10594	**73**	**$500**

Bug Bounty Program

Launched on Feb 2014

Managed by HackerOne **Includes retesting** ? **Bounty splitting enabled** ?

Policy Hacktivity Thanks Updates (32) Collaborators

Rewards

Low	Medium	High	Critical
$100	$500	$3,000	$10,000

Last updated on October 15, 2020. View changes

Policy

Welcome to Yahoo!

Yahoo is a global media and advertising company connecting people to their passions. With one of the largest online audiences in the world, Yahoo brings people closer to what they love — from finance and commerce, to gaming and news — with the trusted products, content and tech that fuel their day. For partners, we provide a full-stack platform to amplify businesses and drive more meaningful connections across advertising, search and media.

We are Paranoid

Our information security team is known as the Paranoids, and we're committed to protecting our brands and our users. As part of this commitment, we invite security researchers to help protect Yahoo and its users by proactively identifying security vulnerabilities via our bug bounty program. Our program is inclusive of all Yahoo brands and offers competitive rewards for a wide array of vulnerabilities. We encourage security researchers looking to participate in our bug bounty program to review our policy to ensure compliance with our rules and also to help you safely verify any vulnerabilities you may uncover.

Table of Contents

- Rules of Engagement
  1. Program Rules
  2. Legal Terms
  3. Safe Harbor

- Responsible Disclosure of Vulnerabilities
  1. Testing
  2. Crafting a Report
  3. Program Scope

- Rewards
  1. Payout Table
  2. Valued Vulnerabilities
  3. Borderline Out-of-Scope, No Bounty

Rules of Engagement

By submitting reports or otherwise participating in this program, you agree that you have read and will follow the Program Rules and Legal Terms sections of this program Policy.

Program Rules

Violation of any of these rules can result in ineligibility for a bounty and/or removal from the program. Three strikes will earn you a temporary ban. Four strikes means a permanent ban.

1. Test vulnerabilities only against accounts that you own or accounts that you have permission from the account holder to test against.
2. Never use a finding to compromise/exfiltrate data or pivot to other systems. Use a proof of concept only to demonstrate an issue.
3. If sensitive information--such as personal information, credentials, etc.--is accessed as part of a vulnerability, it must not be saved, stored, transferred, accessed, or otherwise processed after initial discovery. All copies of sensitive information must be returned to Yahoo and may not be retained.
4. Researchers may not, and are not authorized to engage in any activity that would be disruptive, damaging or harmful to Yahoo, its brands or its users. This includes: social engineering, phishing, physical security and denial of service attacks against users, employees, or Yahoo as a whole.
5. Abide by the program scope. Only reports submitted to this program and against assets in scope will be eligible for monetary award.
6. Researchers may not publicly disclose vulnerabilities (sharing any details whatsoever with anyone other than authorized Yahoo or HackerOne employees), or otherwise share vulnerabilities with a third party, without Yahoo's express written permission.

Legal Terms

In connection with your participation in this program you agree to comply with Yahoo's Terms of Service, Yahoo's Privacy Policy, and all applicable laws and regulations, including any laws or regulations governing privacy or the lawful processing of data.

Yahoo reserves the right to change or modify the terms of this program at any time. You may not participate in this program if you are a resident or individual located within a country appearing on any U.S. sanctions lists (such as the lists administered by the US Department of the Treasury's OFAC).

Yahoo does not give permission/authorization (either implied or explicit) to an individual or group of individuals to (1) extract personal information or content of Yahoo users or publicize this

Yahoo employees (including former employees that separated from Yahoo within the prior 12 months), contingent workers, contractors and their personnel, and consultants, as well as their immediate family members and persons living in the same household, are not eligible to receive bounties or rewards of any kind under any Yahoo programs, whether hosted by Yahoo or any third party.

Safe Harbor

Yahoo will not initiate a lawsuit or law enforcement investigation against a researcher in response to reporting a vulnerability if the researcher fully complies with this Policy.

Please understand that if your security research involves the networks, systems, information, applications, products, or services of another party (which is not us), that third party may determine whether to pursue legal action. We cannot and do not authorize security research in the name of other entities. If legal action is initiated by a third party against you and you have complied with this Policy, we will take reasonable steps to make it known that your actions were conducted in compliance with this Policy.

You are expected, as always, to comply with all applicable laws and regulations.

Please submit a report to us **before** engaging in conduct that may be inconsistent with or unaddressed by this Policy.

Responsible Disclosure of Vulnerabilities

We are continuously working to evolve our bug bounty program. We aim to respond to incoming submissions as quickly as possible and make every effort to have bugs fixed within 90 days of being triaged.

All products and services owned by Yahoo are included in **either** our public or Elite bug bounty program. Please review the program scope before submitting a report. *Elite scope is accessible to invited researchers only.*

Testing

Web traffic to and from Yahoo properties produces petabytes of data every day. When testing, you can make it easier for us to identify your testing traffic against our normal data and the malicious actors out in the world. Please do the following when participating in Yahoo bug bounty programs:

- Where possible, register accounts using your `<username>+x@wearehackerone.com` addresses. **Some of our properties will require this to be eligible for a bounty.**

addition of headers to all outbound requests. Report to us what header you set so we can identify it easily.

Identifier	Format	Example
Your Username	`X-Bug-Bounty: HackerOne-<username>`	`X-Bug-Bounty: HackerOne-flyingtoasters`
Unique Identifier	`X-Bug-Bounty: ID-<sha256-flag>`	`X-Bug-Bounty: ID-6223b07c5323f18b59a70c3ce1b057c56d0eb39de620db6307279deb`
Event Identifier	`X-Bug-Bounty:LiveHackingEvent-<eventid>`	`X-Bug-Bounty: LiveHackingEvent-H1-213`
Tool Identifier	`X-Bug-Bounty: <toolname>`	`X-Bug-Bounty: BurpSuitePro`
Verbose Tool Identifier	`X-Bug-Bounty: <toolname>-version-<version>`	`X-Bug-Bounty: BurpSuitePro-version-2020.1`

When testing for a bug, please also keep in mind:

- Only use authorized accounts so as not to inadvertently compromise the privacy of our users
- When attempting to demonstrate root permissions with the following primitives in a vulnerable process please use the following commands:
  - **Read:** `cat /proc/1/maps`
  - **Write:** `touch /root/<your H1 username>`
  - **Execute:** `id`, `hostname`, `pwd` (though, technically `cat` and `touch` also prove execution)
- Minimize the mayhem. Adhere to program rules at all times. Do not use automated scanners/tools - these tools include payloads that could trigger state changes or damage production systems and/or data.
- Before causing damage or potential damage: Stop, report what you've found and request additional testing permission.

Crafting a Report

- Description of the vulnerability
- Steps to reproduce the reported vulnerability
- Proof of exploitability (e.g. screenshot, video)
- Perceived impact to another user or the organization
- Proposed CVSSv3 Vector & Score (**without** environmental and temporal modifiers)
- List of URLs and affected parameters
- Other vulnerable URLs, additional payloads, Proof-of-Concept code
- Browser, OS and/or app version used during testing

Note: Failure to adhere to these minimum requirements may result in the loss of a reward.

All supporting evidence and other attachments must be stored only within the report you submit. Do not host any files on external services.

Program Scope

Vulnerabilities on a specific brand or web property should be reported to the program to which it is listed "in scope". Please see our detailed scope list at the bottom of this page for a full list of assets that are in scope of this program. This list is subject to change without notice.

To reduce the amount of assets listed in each program we operate, **out of scope** assets are only listed on our public program policy page.
If you've found a vulnerability that affects an asset belonging to Yahoo, but is not included as in scope on any of the Yahoo programs, please report it to this program.

Rewards

You will be eligible for a bounty only if you are the first person to disclose an unknown issue. Qualifying bugs will be rewarded based on severity, to be determined by Yahoo in its sole discretion. Rewards may range from HackerOne Reputation Points and swag to monetary rewards up to $15,000 USD. Awards are granted entirely at the discretion of Yahoo.

At Yahoo's discretion, providing more complete research, proof-of-concept code and detailed write-ups may increase the bounty awarded. Conversely, Yahoo may pay less for vulnerabilities that require complex or over-complicated interactions or for which the impact or security risk is negligible. Rewards may be denied if there is evidence of program policy violations. *A reduction in bounty is also warranted for reports that require specific browser configurations.* Reports in third party software are not eligible for bounties.

Payout Table

Severity	Payout Range
Critical	$10,000 - $15,000
High	$3,000 - $10,000
Medium	$500 - $3,000
Low	$100 - $500
Informative	$0 - $0

Valued Vulnerabilities

All reports will be awarded based on the Common Weakness Enumeration classification. This table provides the CWEs that we will accept, the severity ranges we will classify reports within for the CWE, and some examples of common vulnerability and attack names that we classify within each CWE that we will accept. This table serves only as a guide and the severity classification of a particular vulnerability will be determined by Yahoo in its sole discretion.

Note: Non-listed vulnerabilities may also be eligible. Some vulnerability types may fall under a variety of severity ratings determined by scope/scale of exploitation and impact.

Severity (low)	Severity (high)	CWE-ID	Common Weakness Enumeration	Bug Examples
Low	Medium	CWE-16	Misconfiguration	Subdomain Takeover; Dangling DNS Record; Dangling CNAME Takeover; non-Primary Brand SDTO; DNS Zone Takeover
Critical	Critical	CWE-78	OS Command Injection	Code Injection; LDAP Injection; Remote Code Execution
Low	High	CWE-79	Cross-Site Scripting	Stored XSS; POST-Based XSS; GET-Based XSS; DOM-Based XSS; CSS Injection; Blind XSS
High	Critical	CWE-89	SQL Injection	SQL Injection

Critical	Critical	CWE-91	XML Injection	XML Injection
Medium	Medium	CWE-93	CRLF Injection	CRLF Injection
Critical	Critical	CWE-120	Classic Buffer Overflow	Buffer Overflow
High	Critical	CWE-134	Uncontrolled Format String	Insecure Deserialization
Medium	Critical	CWE-138	Improper Neutralization of Special Elements	Path Normalization
Low	Critical	CWE-200	Information Exposure	User Enumeration with Personal Information; Credentials on GitHub; Confidential Information Exposure; Information Disclosure
Low	High	CWE-203	Information Exposure Through Discrepancy	PHP Admin Information page; MySQL Information page (w/ credentials); Apache Status page
High	Critical	CWE-250	Execution with Unnecessary Privileges	Privilege Escalation to System Account
Medium	Medium	CWE-284	Improper Access Control	Environment Exposure
Low	Low	CWE-304	Missing Critical Step in Authentication	T2 Login Page exposed

Medium	High	CWE-306	Missing Authentication for Critical Function	Exposed Administrative Interface
Informative	Low	CWE-307	Improper Restriction of Excessive Authentication Attempts	Lack of Rate Limiting on Login; CAPTCHA Bypass
Low	Medium	CWE-311	Missing Encryption of Sensitive Data	Cleartext Submission of Passwords
Informative	Low	CWE-327	Use of a Broken or Risky Cryptographic Algorithm	Weak CAPTCHA
Medium	High	CWE-352	Cross-Site Request Forgery	State-Changing CSRF; Non-State-Changing CSRF
Informative	Informative	CWE-359	Privacy Violation	Privacy Violation
Medium	High	CWE-434	Unrestricted Upload of File with Dangerous Type	Unfiltered File Upload
Medium	High	CWE-444	Inconsistent Interpretation of HTTP Requests	HTTP Request Smuggling
Medium	Medium	CWE-494	Download of Code Without Integrity Check	S3 Bucket Upload

Low	Low	CWE-601	Open Redirect	Open Redirect
Critical	Critical	CWE-611	Improper Restriction of XML External Entity Reference	XXE
Low	Low	CWE-706	Use of Incorrectly-Resolved Name or Reference	Incorrectly Resolved Name
High	Critical	CWE-732	Incorrect Permission Assignment for Critical Resource	Horizontal Privilege Escalation; Vertical Privilege Escalation; IDOR (RW, Cross Org); IDOR (RW, Same Org)
Medium	High	CWE-798	Use of Hard-coded Credentials	Hard Coded Credentials
Informative	Critical	CWE-829	Inclusion of Functionality from Untrusted Control Sphere	Server Side Includes Injection; Local File Inclusion; Directory Traversal; Production Host Dependency Confusion; non-Production Host Dependency Confusion
Medium	Critical	CWE-862	Missing Authorization	Horizontal Privilege Escalation; Vertical Privilege Escalation; IDOR (RO, Same Org); IDOR (RO, Cross Org)
Informative	High	CWE-863	Incorrect Authorization	Authorization Bypass; Account Takeover; Social Media Takeover (Brand, <12mo, w/creds); Social Media (w/o creds)

Medium	Critical	CWE-918	Server-Side Request Forgery	Semi-Blind SSRF (Service level); Semi-Blind SSRF (Host level); Semi-Blind SSRF (File Contents); Semi-Blind SSRF (File Existence); Unrestricted SSRF; Content-Restricted SSRF (Multiple); Content-Restricted SSRF (Single)
Low	Low	CWE-941	Incorrectly Specified Destination in a Communication Channel	Incorrect Destination

Borderline Out-of-Scope, No Bounty

These issues are eligible for submission, but not eligible for bounty or any award. Once triaged, they will be closed as `Informative` only if found to be valid or `Spam` if found to be not valid. When reporting vulnerabilities, please consider (1) attack scenario / exploitability, and (2) security impact of the bug.

Any non-Yahoo Applications	"Self" XSS
Missing Security Best Practices	HTTP Host Header XSS
Confidential Information Leakage	Clickjacking/UI Redressing
Use of known-vulnerable library (without proof of exploitability)	Intentional Open Redirects
Missing cookie flags	Reflected file download
SSL/TLS Best Practices	Incomplete/Missing SPF/DKIM
Physical attacks	Social Engineering attacks
Results of automated scanners	Login/Logout/Unauthenticated CSRF
Autocomplete attribute on web forms	Using unreported vulnerabilities
"Self" exploitation	Issues related to networking protocols

Verbose error pages (without proof of exploitability)	Denial of Service attacks
Yahoo software that is End of Life or no longer supported	Account/email Enumeration
Missing Security HTTP Headers (without proof of exploitability)	Internal pivoting, scanning, exploiting, or exfiltrating data

Note: 0-day and other CVE vulnerabilities may be reported 30 days after initial publication (CVE List Status of `Published`). We have a team dedicated to tracking CVEs as they are released; hosts identified by this team and internally ticketed will not be eligible for bounty.

Do Not Report

The following issues are considered out of scope:

- Those that resolve to third-party services
- Issues that do not affect the latest version of modern browsers
- Issues that we are already aware of or have been previously reported
- Issues that require unlikely user interaction
- Disclosure of information that does not present a significant risk
- Cross-site Request Forgery with minimal security impact
- CSV injection
- General best practice concerns
- All Flash-related bugs

Special Situations

Same Bug, Different Host

For each report, please allow Yahoo sufficient time to patch other host instances. If you find the same bug on a **different** (unique) host, prior to the report reaching a `triaged` state, file it within the existing report to receive an additional 5% bonus (per host, not domain). Any reports filed separately *while we are actively working to resolve the issue* will be treated as a `duplicate`.

Same Bug, Different Path

For each report, please allow Yahoo sufficient time to patch related paths. If you find the same bug on a **different** (unique) path, prior to the report reaching a `triaged` state, file it within the existing report to receive an additional 5% bonus (per path). Any reports filed separately *while we are actively working to resolve the issue* will be treated as a `duplicate`.

the same vulnerability across different parameters of a resource, or demonstrations of multiple attack vectors against a fundamental framework issue. We kindly ask you to consolidate reports rather than separate them.

Note: Additional payloads, parameters, hosts and paths will not receive multiple bonuses.

Last updated on October 19, 2021. View changes

Scopes

In Scope

Domain	**data.mail.yahoo.com**	Critical	$ Eligible
Domain	**le.yahooapis.com**	Critical	$ Eligible
Domain	**onepush.query.yahoo.com**	Critical	$ Eligible
Domain	**proddata.xobni.yahoo.com**	Critical	$ Eligible
Domain	**apis.mail.yahoo.com**	Critical	$ Eligible
Domain	**yimg.com** yimg is a resource storage and content distribution network (CDN). **Note:** Reports submitted that exploit bugs **only** in the context of the `yimg.com` domain are most likely to be closed as `Informative`. Most bugs in `*.yimg.com` will require a proof-of-concept or proof-of-exploit that escalates into one of the primary brand or product domains (e.g. yahoo.com or aol.com) to be eligible for bounty. CVSS Environmental scores have been set to account for this limitation. What does that mean for my report? 1. If you show escalation into a trusted domain's context (such as yahoo.com) it will be accepted at 100% bounty rate. A bonus may be applied for different instances within the trusted domain list only; not for other instances of vulnerabilities content on yimg.com.	Medium	$ Eligible

	is removed. There are no "same bug different host" or other vulnerability grouping bonus offers for this asset.		
Source code	Arkime **Review the Code** • Source Code • Submit a PR to fix/update the code - fork the codebase then submit a PR • Visit our web page at https://arkime.com/ for pre-bulit rpm/deb and instructions for running yourself. **Out of Scope** • Known unauthenticated endpoints such as `parliament.json` & `eshealth.json` • UI based bugs on `parliament` • demo.arkime.com • *.molo.ch (old website)	Critical	$ Eligible
Source code	Athenz **Review the Code** • Source Code • Submit a PR to fix/update the code - fork the codebase then submit a PR **Out of Scope** `yahoo/athenz/ui`, `yahoo/athenz/contributions`, and `yahoo/athenz/docker` are outdated from our own internal deployment because of our use of Okta and Duo which we are not able to deploy to you all for this event; this is why we stated the Athenz UI was out of scope during the scoping call. The UI was just given out as a starting point so whoever needs it, can take it, integrate with their own authentication system and also provide all the necessary protections. Our UI devs worked with the Paranoids' red team internally for quite some time to go through all this, addressing many different types of bug classes with our integration with Okta and Duo and that's what we're running in our production instance.	Critical	$ Eligible
Other	**Yahoo! (misc)**	Critical	$ Eligible

	Bugs with Yahoo! that are not listed in scope of our other Yahoo-related assets can still be submitted to this asset and ***might*** be eligible for award, at the sole discretion of the Verizon Media Bug Bounty team.		
Other	**7News** • 7News iOS • 7News Android	Critical	$ Eligible
Other	**Yahoo Sports: Editorial** **In Scope** • https://sports.yahoo.com/ • https://api-secure.sports.yahoo.com **Out of scope** • shop.yahoosports.com (Third party)	Critical	$ Eligible
Other	**Yahoo Sports: Fantasy Sports** **In Scope** • Yahoo Fantasy Sports Android • Yahoo Fantasy Sports iOS • Yahoo Fantasy Sports (web) • https://sports.yahoo.com/odds/ **Notes** The betting feature in Fantasy is provided by a third party, BetMGM. `https://sports.yahoo.com/odds/`, is the page from where it redirects the user to the BetMGM. This is geographically restricted.	Critical	$ Eligible
Other	**Yahoo Sports: Rivals** **In Scope** • https://n.rivals.com • https://www.rivals.com/ **Notes** All testing against rivals is to be **MANUAL only.** ZERO automated tools are allowed. **This notice is your warning.**	Critical	$ Eligible

	• *.rivalscampseries.com (3rd party) • Rivals iOS		
Other	**Yahoo Finance** • iOS • Android • *.finance.yahoo.com • OBI Premium Checkout: https://checkout.finance.yahoo.com/checkout/v1 • API WebSockets Streaming Market Data: http://streamer.finance.yahoo.com • finance.mobile.yahoo.com • finance.query.yahoo.com	Critical	$ Eligible
Other	**Yahoo HK Auctions** • Yahoo HK Auctions Android • Yahoo HK Auctions iOS • Yahoo HK Auctions (web)	Critical	$ Eligible
Other	**Yahoo HK News** • Yahoo HK News Android • Yahoo HK News iOS	Critical	$ Eligible
Other	**Yahoo HK Shopping** **In Scope** • Yahoo HK Shopping Android • Yahoo HK Shopping iOS • Yahoo HK Shopping (web) **Out of Scope** • yahooshopping.myguide.hk	Critical	$ Eligible
Other	**Yahoo Live Web Insights** • Yahoo Live Web Insights iOS	Critical	$ Eligible
Other	**Yahoo Mail** • Yahoo Mail Android • Yahoo Mail AndroidGo • Yahoo Mail FireOS • Yahoo Mail iOS • Yahoo Mail (web) Out of Scope:	Critical	$ Eligible

Other	**Yahoo Search** • Yahoo Search Android • Yahoo Search iOS • Yahoo Search (web)	Critical	$ Eligible
Other	**TW eCommerce: Auctions** **In Scope** • Yahoo TW Auctions Android • Yahoo TW Auctions iOS • Yahoo TW Auctions: • *.bid.yahoo.com • https://tw.bid.yahoo.com • Yahoo TW Auctions APIs: • https://tw.bid.yahoo.com/api/ • https://tw.api.bid.yahoo.com:4443 • Search API: tw.search.ec.yahoo.com **Notes** • Access to the Taiwan sites from some countries in Europe may be blocked. • `Buyer` accounts can be set up for any Yahoo user. • `Seller` accounts require a TW phone number and 2FA. • **Do not** use fake data (like nid) when operating the cash functions, it may cause real money to be stuck; **we will hold you accountable for broken workflows.** • You are required to clean up all the testing data related to posting new products. • You **must** include the following “test” label in **ALL** posts (in the most visible location) to prevent regular users from interacting with hacker-created content: `[PARANOIDS-勿下標][TEST]` -- *Any reports identified that are missing this label, will not receive a bounty.* **Out of Scope** • *.yahoo.com.tw • ismarus-ap-94600.tw.juiker.net • *.tw.juiker.net • auth.tw.juiker.net/oauth2/getUserTokenByTurnkey • *.straas.net	Critical	$ Eligible

Other	**TW Media: News** **In Scope** - Yahoo TW News Android - Yahoo TW News iOS - Yahoo TW News - *.tw.news.yahoo.com - Backend API: https://news-app.abumedia.yql.yahoo.com:443/ - Web: https://tw.news.yahoo.com - Content API: https://ncp-gw-abu.media.yahoo.com/ **Out of Scope** - news.campaign.yahoo.com.tw - *.yahoo.com.tw	Critical	$ Eligible
Other	**TW eCommerce: Shopping** **In Scope** - Yahoo TW Shopping Android - Yahoo TW Shopping iOS - Yahoo TW Shopping - twpay.buy.yahoo.com - Web: https://tw.buy.yahoo.com/ - Mobile Web: https://m.tw.buy.yahoo.com/ - API: https://tw.mapi.shp.yahoo.com - Search API: tw.search.ec.yahoo.com - Rushbuy API: rushbuy.buy.yahoo.com **Out of Scope** - *.yahoo.com.tw - iOS: TPDirect.framework - Android: tech.cherri.tpdirect.api	Critical	$ Eligible
Other	**TW Media: Stock** **In Scope** - Yahoo TW Stock Android - Yahoo TW Stock iOS - Yahoo TW Stock - tw.stock.yahoo.com - API: https://stock-app.abumedia.yql.yahoo.com	Critical	$ Eligible

	• `stock.yahoo.com` and `finance.yahoo.com` are identical; Reports will NOT be credited same-bug-different-host bonuses when issues are found on both domains. • TW Stock Apps have a strong dependency with third party SDK(s) for receiving the real-time quote data in the market. Every page containing values (volume, prices, up/down flag, ...) of index, tickers, etfs, ... , ticker information, line chart, notifications setting are all from the SDK. And the connection with the SDK service is established when the app launches and lasts the app's whole lifetime. **These SDK service(s) are out of scope.** **Out of Scope** • *.yahoo.com.tw • tw.finance.yahoo.com • Quote SDK (from Systex inc.)		
Other	**TW eCommerce: Store** **In Scope** • Yahoo TW Store Android • Yahoo TW Store iOS • Yahoo TW Store ◦ *.tw.mall.yahoo.com ◦ m.mall.yahoo.com ◦ Web: https://tw.mall.yahoo.com/ ◦ Mobile Web: https://m.tw.mall.yahoo.com/ ◦ API: https://tw.ews.mall.yahooapis.com/ • Search API: tw.search.ec.yahoo.com **Out of Scope** • *.yahoo.com.tw	Critical	$ Eligible
Other	**Yahoo Video** • Yahoo Video FireTV • Yahoo Video tvOS	Critical	$ Eligible
Other	**Yahoo Weather** • Yahoo Weather Android • Yahoo Weather iOS • Yahoo Weather (web)	Critical	$ Eligible

	- *.flurry.com		
Other	Newsroom - Newsroom Android - Newsroom iOS - Newsroom (web)	Critical	$ Eligible
Other	Yahoo News - *.news.yahoo.com - yahoo.com/news	Critical	$ Eligible
Other	Gemini - *.gemini.yahoo.com - *.admanager.yahoo.com - monetization.flurry.com	Critical	$ Eligible
Other	Makers - *.makers.com	Critical	$ Eligible
Other	BUILD - *.buildseries.com	Critical	$ Eligible
Other	Built By Girls **In Scope** - *.builtbygirls.com **Notes** - You MUST register for an account with your `@wearehackerone` email address or else your report will NOT be eligible for bounty. **Out of Scope** - jobs.builtbygirls.com (3rd party, Jobboard.io) - store.builtbygirls.com (3rd party, BrightStores) - builtbygirls.mybrightsites.com (3rd party, BrightStores)	Critical	$ Eligible
Other	Membership **In Scope** - https://login.yahoo.com - https://login.aol.com - https://api.login.yahoo.com	Critical	$ Eligible

https://developer.yahoo.com/oauth2/guide/

Specific paths to target....
For `login.*.com`

- /account/logout
- /auth/2.0/credentials
- /auth/1.0/
- /saml2/
- /account
- /oauth2
- /ylc
- /account/challenges
- /account/access
- /oauth2/device_auth
- /ctv
- /activate
- /forgot

For `api.login.*.com`

- /api
- /oauth2/get_token
- /oauth2/web_session
- /oauth2/device_sessions
- /oauth2/device_authorization
- /oauth2/device_auth
- /oauth2/revoke
- /oauth2/introspect

Out of Scope

- Any rate limits for authentication attempts.
- Any differentiated treatment based on account, browser, IP address etc.

Limits

- Limit traffic against our services to < 10/second when probing or testing.

Other	**Omega** `*omega*.yahoo.com`	Critical	$ Eligible
Other	**Ensemble** `*ensemble*.yahoo.com`	Critical	$ Eligible

- *.caldav.calendar.yahoo.com

Specific paths to look at:

- https://calendar.yahoo.com/ws/v3/users/
- https://caldav.calendar.yahoo.com/principals/users/
- https://caldav.calendar.yahoo.com/dav/*/calendar/

Limits

Limit traffic against our services to < 10/second when probing or testing.

Other

RYOT

In Scope

- RYOT Mobile SDK (iOS and Android) `https://s.yimg.com/cv/apiv2/ar_sdk/*
- *.ryot.org (site under construction)

Notes

- The RYOT Augmented Reality SDK is used by our major mobile apps.
- `ryot.org` is hosted on WordPress; WP's services are not in scope

Out of Scope

- *.ryotfilms.com (third party)
- *.ryot.com (third party)
- *.portal.ryot.com (third party)

Critical

$ Eligible

Other

Engadget

In Scope

- APIs
- *.engadget.com

Notes

- Separate reports for the same or similar payload/issue against multiple international editions, will be marked as duplicates and paid only once for Engadget international editions.

Out of Scope

Critical

$ Eligible

	• *.japanese.engadget.com (Engadget International Edition) • jobs.engadget.com (3rd party, Jobboard.io)		
Other	**TechCrunch** **In Scope** • *.techcrunch.com • Custom endpoints: `https://techcrunch.com/wp-json/tc/v1/*` -- These are custom endpoints that use the WordPress architecture and output methods but modified for our uses with custom data. • Custom mobile endpoints: `https://techcrunch.com/wp-json/tc/mobile/v2/*` -- These are the endpoints that are used by the mobile apps to retrieve posts for the apps. • Default WordPress: `https://techcrunch.com/wp-json/wp/v2/*` -- We also leverage most of WordPress' out of the box endpoints with added custom data to augment the output. **Out of Scope** • *.crunchbase.com (3rd party, Crunchbase) • *.tc-appunite.herokuapp.com (3rd party, Heroku now closed) • *.parsely.com (3rd party, Parse.ly) • *.swiftype.com (3rd party, Swiftype now closed) • *.marketo.com (3rd party, Marketo) • *.urbanairship.com (3rd party, Urban Airship) • *.sailthru.com (3rd party, Sailthru) • *.spot.im (3rd party, Spot.IM) • *.tcdisrupt.com (3rd party, App) • *.bit.ly (3rd party, Bit.ly) • *.thomsonreuters.com (3rd party, Open Calais) • *.tinypass.com (3rd party, Piano/Tinypass)	Critical	$ Eligible
Other	**Autoblog** **In Scope** • www.autoblog.com **Out of Scope** • *.spot.im (3rd party, Spot.IM)	Critical	$ Eligible

Other	AOL Mail **In Scope** • *.mail.aol.com (see exclusions below) • rpc.mail.aol.com **Notes** • oidc.mail.aol.com (Hosted by Mail, but belongs to `Membership`) **Out of Scope** • mail.aol.com/calsvc • AOL iOS • AOL Android • AOL FireOS • AOL Desktop Gold • apis.mail.aol.com • test-apis.mail.aol.com • *.aolmail.com • mail.aol.com/classicab • mail.aol.com/getmydata • mail.aol.com/ws • *.aol.com	Critical	$ Eligible
Other	Yahoo Sports: Rivals Forums **In Scope** • *.forums.rivals.com **Notes** • All testing against rivals is to be **MANUAL only.** ZERO automated tools are allowed. **This notice is your warning.** • This is third party software and will be awarded at a 50% bounty rate. • Reports on this asset will not be eligible for bonuses.	Critical	$ Eligible
Other	Yahoo Sports: Mobile • Yahoo Sports Android • Yahoo Sports iOS • *.protrade.com	Critical	$ Eligible
Other	Yahoo Sports: Fantasy Slate/PicknWin	Critical	$ Eligible

Other	**Yahoo Sports: Best Ball** **In Scope** • https://bestball.fantasysports.yahoo.com/	Critical	$ Eligible
Other	**Yahoo Sports: Fantasy Games** **In Scope** • https://sports.yahoo.com/fantasy/ • Fantasy Basketball • Fantasy Hockey • Fantasy User Profiles • Fantasy Football (out of season) • Public cookie-based API endpoints (used by some FE stacks) • Public OAuth2 endpoints • tournament.fantasysports.yahoo.com **Out of Scope** • *.sendbird.com (Third Party, SendBird)	Critical	$ Eligible
Other	**Yahoo Sports: Fantasy Wallet** **In Scope** • https://sports.yahoo.com/dailyfantasy/account/addfunds	Critical	$ Eligible
Other	**Yahoo Sports: Daily Fantasy** **In Scope** • https://sports.yahoo.com/dailyfantasy/ • https://sports.yahoo.com/dailyfantasy/contest/create	Critical	$ Eligible
Other	**Social Media Accounts** **Requirements** • Account in question has posted content within 365 days of report submission • Account in question is related to a company, brand, or product • Exposed (valid/functional/active) credentials that allow login to an account **In Scope**	Critical	$ Eligible

	Note: “Account in question” means the account you are reporting as “vulnerable.” **Out of Scope** • Account in question is related to an individual (employee, freelancer or otherwise) • Brute forcing account credentials		
Other	**TW Media: Front Page** **In Scope** • tw.mobi.yahoo.com • tw.yahoo.com • Content API: https://ncp-gw-abu.media.yahoo.com/ **Out of Scope** • *.yahoo.com.tw	Critical	$ Eligible
Other	**TW eCommerce: Used Car** **In Scope** • tw.usedcar.yahoo.com **Notes** Refer to the **Notes** section in the `TW eCommerce: Auctions` listing. **Out of Scope** • *.yahoo.com.tw • autos.yahoo.com.tw • tw.serviceplus.yahoo.com	Critical	$ Eligible
Other	**Media Platform Marketing Website** **In Scope** • *.verizondigitalmedia.com • www.verizondigitalmedia.com (prod) • stage-www.verizondigitalmedia.com (staging, only non-english content) • research.verizondigitalmedia.com **Notes**	Critical	$ Eligible

company/request-support/ our-company/customer-support/)

Out of Scope

- *.verizonmedia.com (Company home page)
- info.verizondigitalmedia.com (Third Party, Pardot/Salesforce)
- status.verizondigitalmedia.com (Third Party, Status.io)

The pages listed under these URL paths (Third Party, instapage.com):

- www.verizondigitalmedia.com/announcement/*
- www.verizondigitalmedia.com/campaign/*
- www.verizondigitalmedia.com/case-study/*
- www.verizondigitalmedia.com/e-book/*
- www.verizondigitalmedia.com/free-trial/*
- www.verizondigitalmedia.com/infographic/*
- www.verizondigitalmedia.com/internal/*
- www.verizondigitalmedia.com/landing/*
- www.verizondigitalmedia.com/platform-updates/*
- www.verizondigitalmedia.com/referral/*
- www.verizondigitalmedia.com/report/*
- www.verizondigitalmedia.com/rsvp/*
- www.verizondigitalmedia.com/television-academy/*
- www.verizondigitalmedia.com/webinar/*
- www.verizondigitalmedia.com/white-paper/*

Other

Media Platforms Engineering Blog

In Scope

- eng.verizondigitalmedia.com
- eng-staging.verizondigitalmedia.com

Notes

Bugs present on both Staging and production will not be awarded `Same Bug Different Host` bonus.

Critical

$ Eligible

Other

AOL (misc)

Critical

$ Eligible

In Scope

- *.aol.com

Notes

AOL-related assets can still be submitted to this asset and ***might*** be eligible for award, at the sole discretion of the Verizon Media Bug Bounty team.

Out of Scope

- *nat.aol.com
- *.ipt.aol.com

Other

AOL Homepage

Critical

$ Eligible

In Scope

- www.aol.fr
- www.aol.de
- www.aol.co.uk
- www.aol.jp
- www.aol.in
- www.aol.ca
- www.aol.com
- www.aol.com/*
- AOL Games Landing Page - https://www.aol.com/games/ -> **see 3rd Party Notes Below**

Notes

OOS Exception: 3rd party components that affect aol.com (e.g. XSS executes in AOL.com domain resulting from abuse of TravelZoo module on Travel page)

Out of Scope

First Party Things:

- https://ottr.video.yahoo.com/v1/video-exp/schedule
- https://s.yimg.com/rb/screwdriver/ctv/ve-module/builds/prod/aol/dist/vem.js

Second Party Things:

- DataMask by AOL (White Label app)
- AOL OnePoint (White Label app)
- Private WiFi by AOL (White Label app)
- AOL Games (White Label app)

	`Conversations for You`, Commenting on articles (and more) (Third Party, OpenWeb) • spot.im (Third Party, OpenWeb) • Individual AOL Games pages are rendered by us, but we iFrame in the Masque game urls. (Third Party, Masque) • games.com, fungames.aol.com & fungames.com (Third Party, Masque) • Comparecards.aol.com is CNAME'd to our own ATS cluster which forward maps requests to the comparecards cloudfront distribution. (Third Party, CompareCards) • JS widget on the AOL.com homepage providing news stories. (Third Party, Zergnet) • Serverside rendered module on aol.com/real-estate, data comes from Zillow api. (Third Party, Zillow) • Serverside rendered module on www.aol.com/travel, data comes from TravelZoo api. (Third Party, Travel Zoo) • rezserver.com (Third Party, Travel Zoo)		
Other	AOL Mobile Apps **Out of Scope** • Apps from the app stores are not in scope.	Critical	$ Eligible
Other	AOL Search **In Scope** • search.aol.ca • search.aol.co.uk • search.aol.com • recherche.aol.fr • suche.aol.de **Notes** Any bugs found in non-production environments will **not** be eligible for the `Same Bug Different Host` bonus if the issue also exists in production.	Critical	$ Eligible
Other	AOL Help **In Scope** • help.aol.com • assistance.aol.fr	Critical	$ Eligible

Any bugs found in non-production environments will **not** be eligible for the `Same Bug Different Host` bonus if the issue also exists in production.

Out of Scope

- assist.aol.com (2nd party service)
- helpisp.netscape.com
- helpconnect.netscape.com
- help.compuserve.com

Other

Yahoo Elections

Critical

$ Eligible

In Scope

Note: you MUST include the `ref=electionsNight` *parameter to hit the right in-scope pages.*

- https://www.yahoo.com/elections?ref=electionsNight
- https://www.yahoo.com/elections/senate?ref=electionsNight
- https://www.yahoo.com/elections/house?ref=electionsNight
- https://www.yahoo.com/elections/state/al?ref=electionsNight (and all other US state pages)

Notes

Any bugs found in non-production environments will **not** be eligible for the `Same Bug Different Host` bonus if the issue also exists in production.

Out of Scope

- elections.yahoo.com (First Party, Yahoo Search)
- yahoo.com/elections (First Party, Yahoo Search)
- yahoo.turbovote.org (Third Party, Turbovote)
- Historical Race Feed: https://www.realclearpolitics.com/poll/race/903/historical_data.json (Third Party, Real Clear Politics)
- Presidential RCP Feed: https://www.realclearpolitics.com/syn/verizon_2020_president_trump_vs_/main.json (Third Party, Real Clear Politics)
- Trump Approval RCP Feed: https://www.realclearpolitics.com/syn/verizon_presi

	0_senate/main.json (Third Party, Real Clear Politics) • House RCP Feed: https://www.realclearpolitics.com/syn/verizon_house_2020/main.json (Third Party, Real Clear Politics) • Associated Press, Third Party • Scribble Live, Third Party		
Other	**IDS** **In Scope** • id.vdms.io **Notes** Pre-production domains will **not** be eligible for `Same Bug Different Host` bonuses. These include: • id-stg.vdms.io • id-dev.vdms.io • stg2-identity-dashboard.identity.vdms.io • dev-identity-dashboard.identity.vdms.io • ci-identity-dashboard.identity.vdms.io **Out of Scope** • manage.vdms.io	Critical	$ Eligible
Other	**Online Marketplace** Online Marketplace (MyAccount) supports many AOL properties and can be accessed by a variety of CNAME records. • billupdate.aol.com • myaccount.aol.com • myservices.aol.com • payments.aol.com • mybenefits.aol.com • cancel.aol.com • bill.aol.com Please consolidate your reports. **Note: Reporting the same issue separately for multiple CNAMEs will result in reports being marked as `Duplicate` at best.**	Critical	$ Eligible
Other	**AOL Publishers**	Critical	$ Eligible

Other	**In Scope** • *.isp.netscape.com • *.lite.aol.com • *.compuserve.com • www.wmconnect.com Other places to look • webaccelerator.isp.netscape.com • register.isp.netscape.com • admin.isp.netscape.com • www.getnetscape.com • netscape.compuserve.com **Out of Scope** • Subdomains of `wmconnect.com` outside of `www` **Notes** • These services are designed for delivery through slow internet connections. • Registration for these services has been disabled. • Help-related pages/domains should be reported to the AOL Help asset.	Critical	$ Eligible
Other	**DSP** **In Scope** • api-v3.admanagerplus.yahoo.com • admanagerplus.yahoo.com **Notes** Restrict your rate limit on requests to `120 requests/minute` to prevent yourself being auto-banned or impacting our production system. This asset is not in eligible for bounty through our public bug bounty program.	Critical	$ Eligible
Android: Play Store	**com.yahoo.mobile.client.android.mail** • Yahoo Mail Android • Yahoo Mail AndroidGo • Yahoo Mail FireOS • Sign up for the Beta here	Critical	$ Eligible

Source code	**Yahoo Open Source Projects (misc)** Select open source projects are now eligible for bounties! The rest of our open source projects are technically in scope, but at a reduced rate for the time being.	Critical	Ineligible
Other	**Other (misc)** Only use this asset when nothing else can be reasonably selected. Bugs with Yahoo products that are not listed in scope of our Public Program can still be submitted to this asset and *might* be eligible for award, at the sole discretion of the Yahoo Bug Bounty team . Use this asset for: • *.vzbuilders.com • *.oath.cloud • *.yahoo.cloud	Critical	Ineligible
Other	**EdgeCast - Customers** Self-registered accounts will be limited to demonstration zones and are subject to automatic blocks or removal. This asset is not eligible for bounty through our public bug bounty program. • my.edgecast.com • api.edgecast.com/v2/mcc	Critical	Ineligible
Other	**EdgeCast - Partners** Self-registered accounts will be limited to demonstration zones and are subject to automatic blocks or removal. This asset is not eligible for bounty through our public bug bounty program. • partner.edgecast.com • api.edgecast.com/v2/pcc	Critical	Ineligible
Other	**Uplynk** • *.downlynk.com • *.uplynk.net • *.uplynk.com This asset is not in eligible for bounty through our public bug bounty program.	Critical	Ineligible

Domain	*.yahoo.net
Domain	***.yahoo.com.tw**
Other	**Yahoo Cricket** - Yahoo Cricket Android - Yahoo Cricket iOS - Out of Scope: `cricket.yahoo.net` (third party) - Out of Scope: `*.sportz.io` (third party)
Other	**Yahoo 7** - au.yahoo.com - nz.yahoo.com
Other	**Boundless** To submit bugs, contact: yj-csirt@mail.yahoo.co.jp This includes these and possibly other domains currently and/or formerly associated with Yahoo Japan: - *.yahoo-net.jp - *.yahoo.net
Other	**Miscellaneous** - *.aolcdn.com - *.yahoo.com.hk - Media Group One - Movies Hong Kong - Onwander - Volicon - Volicloud - Yahoo Operated WordPress blogs - files.molo.ch
Other	**Historical + Divestitures** This is a list of products and companies which were previously owned but have been shut down or sold and are not in scope of **Yahoo.** - About.me - Flickr - Go90 - MovieFone - Oath: Impact - HuffPost - Patch Media

- Winamp
- Yahoo Answers
- Yahoo Groups
- Yahoo Play
- Yahoo Together (Squirrel)
- Yahoo Messanger
- Yahoo Small Business
- Yahoo TW eSports
- Yahoo Japan

Other

SSRF Test Servers (information)

SSRF Test Servers

If you think you've got an SSRF attack against our network, please use these two groups of servers to prove it to us. There's a whole bunch of different file formats on these servers and they're all identical. To prove your SSRF, please send your attacks in a way that attempt to read or write content to/from one of these servers in each network segment (Prod + Corp). The difference between each host within each category is just their geolocation, which in most circumstances does not matter what you target. HTTPS is also enabled on these servers.

Production Network

- banana.stand.ne1.prod.oath (banana.stand.ne1.yahoo.com)
- banana.stand.gq1.prod.oath (banana.stand.gq1.yahoo.com)
- banana.stand.bf1.prod.oath (banana.stand.bf1.yahoo.com)
- banana.stand.bf2.prod.oath (banana.stand.bf2.yahoo.com)
- banana.stand.sg3.prod.oath (banana.stand.sg3.yahoo.com)
- banana.stand.ir2.prod.oath (banana.stand.ir2.yahoo.com)
- banana.stand.tw1.prod.oath (banana.stand.tw1.yahoo.com)
- banana.stand.tp2.prod.oath (banana.stand.tp2.yahoo.com)

Corporate Network

- banana.stand.corp.gq1.cic.oath (banana.stand.cgq1.yahoo.com)
- banana.stand.corp.bf1.cic.oath (banana.stand.cbf1.yahoo.com)
- banana.stand.corp.sg3.cic.oath (banana.stand.csg3.yahoo.com)
- banana.stand.corp.ne1.cic.oath (banana.stand.cne1.yahoo.com)

Files to target take the filename format of `<extension>_###.<extension>`. For example: `txt_001.txt` and `zip_001.zip`. We've put up a bunch of different file formats that can be targeted for your testing needs. There is one other file that is simple text, but does not have a file extension, reach that by asking for `noext_01`.

File types available include:
avi, bmp, css, csv, doc, docx, dtd, flv, gif, html, icns, ics, ico, jar, jpg, js, json, md, mkv, mov, mp3, mp4, odp, ods, odt, ogg, pdf, php, png, ppt, rss, svg, tiff, txt, wav, wmv, xls, xlsx, xml, xsl, zip

`http://<hostname>/hackerone-<username>` so that we can identify **your** activity in the logs more easily.

When submitting a report (in addition to all the usual details) please make sure to:

1. Attach a copy of the file you fetched.
2. Include the timestamp you fetched the file.
3. Note the SSRF server that you fetched the file from.

The Fine Print

If you can't hit these servers but can hit something else inside our network, you must provide a working POC and understand that we will individually evaluate impact of the host you tested with.

We reserve the right to award a $0 bounty for any SSRF (or similar) reports that are not able to touch these servers.

Also, we will periodically review the logs on these servers and may reach out to hackers that have hit the server but not submitted a report. If this happens, you will be eligible for **a maximum award of 10%** for the report.

Other

Challenge Coins

These are just for fun.

- H1-213-2019
- [H1-415-2020](coming soon)
- [H1-2004-2020](coming soon)

Other

Umbrella Out of Scope List

Any other reference to out of scope items in this policy or scope still apply. Verizon Media reserves the right to award or not award on assets that may not yet be on this list or in this policy.

ALL THE FOLLOWING ASSETS ARE OUT OF SCOPE

- AOL Mail
  - AOL Desktop Gold
  - apis.mail.aol.com
  - test-apis.mail.aol.com
  - *.aolmail.com
  - mail.aol.com/classicab
  - mail.aol.com/getmydata
  - mail.aol.com/ws
  - mail.aol.com/calsvc

- Athenz Source Code
  - yahoo/athenz/ui

  - *.spot.im (3rd party, Spot.IM)
  - Development-like environments for autoblog.com exist, but should not be tested; keep the testing in Production (www.).

- Built By Girls
  - jobs.builtbygirls.com (3rd party, Jobboard.io)
  - store.builtbygirls.com (3rd party, BrightStores)
  - builtbygirls.mybrightsites.com (3rd party, BrightStores)

- *.vdms.com
- EdgeCast
  - Customers
  - Partners
  - Wholesalers

- Engadget
  - *.spot.im (3rd party, Spot.IM)
  - *.cn.engadget.com (Engadget International Edition)
  - *.chinese.engadget.com (Engadget International Edition)
  - *.japanese.engadget.com (Engadget International Edition)
  - jobs.engadget.com (3rd party, Jobboard.io)

- Historical & Divestitures
  - About.me
  - Flickr
  - Go90
  - MovieFone
  - Patch Media
  - PawNation
  - Polyvore
  - Shoutcast
  - Style Me Pretty
  - Winamp
  - Yahoo Together (Squirrel)
  - Yahoo Play
  - Yahoo TW eSports
  - The Huffington Post
    - news.huffingtonpost.com (3rd party, CampaignMonitor)
    - coupons.huffpost.com (3rd party, Groupon)
    - huffpost.atlassian.net (3rd party, Atlassian)
    - huffpoststuff.com (3rd party, StackCommerce)
    - subscribe.huffpost.com (3rd party, Epsilon)

- Miscellaneous
  - *.aolcdn.com

  - Volicon
  - Volicloud
  - Yahoo Operated WordPress blogs
  - Files.molo.ch
  - sg.auctions.yahoo.com (3rd party, GMarket)

- Moloch Source Code
  - Known unauthenticated endpoints such as parliament.json & eshealth.json
  - www.molo.ch
  - demo.molo.ch
  - *.molo.ch (production website)
  - UI based bugs on parliament

- RYOT
  - *.ryotfilms.com (third party)
  - *.ryot.com (third party)
  - *.portal.ryot.com (third party)

- *.spot.im
- TechCrunch
  - *.crunchbase.com (3rd party, Crunchbase)
  - *.tc-appunite.herokuapp.com (3rd party, Heroku now closed)
  - *.parsely.com (3rd party, Parse.ly)
  - *.swiftype.com (3rd party, Swiftype now closed)
  - *.marketo.com (3rd party, Marketo)
  - *.urbanairship.com (3rd party, Urban Airship)
  - *.sailthru.com (3rd party, Sailthru)
  - *.spot.im (3rd party, Spot.IM)
  - *.tcdisrupt.com (3rd party, App)
  - *.bit.ly (3rd party, Bit.ly)
  - *.thomsonreuters.com (3rd party, Open Calais)
  - *.tinypass.com (3rd party, Piano/Tinypass)

- TW eCommerce: Auctions
  - *.yahoo.com.tw
  - ismarus-ap-94600.tw.juiker.net
  - *.tw.juiker.net
  - auth.tw.juiker.net/oauth2/getUserTokenByTurnkey
  - *.straas.net
  - iOS: JuikerIMSDK.framework, StraaS-iOS-SDK
  - Android: io.straas.android.sdk
  - ecfme.famiport.com.tw (Third Party)

- TW eCommerce: Shopping
  - *.yahoo.com.tw
  - iOS: TPDirect.framework

  - *.yahoo.com.tw

- Uplynk (VDMS)
- Verizon
  - MapQuest
    - MapQuest Android
    - MapQuest FireOS
    - MapQuest iOS
    - *.mapquest.com
  - MovilData
  - Skyward
  - XO
  - *.verizonwireless.com
  - *.verizon.com
  - *.verizon.net
  - *.vzw.com
  - *.myvzw.com
  - *.verizonbusiness.com
- vzbuilders
  - smart.vzbuilders.com
  - some other vzbuilders sub domains
- Yahoo 7
  - au.yahoo.com
  - Nz.yahoo.com
- Yahoo Answers
- Yahoo Cricket
  - Yahoo Cricket Android
  - Yahoo Cricket iOS
  - Out of Scope: cricket.yahoo.net (third party)
  - Out of Scope: *.sportz.io (third party)
- Yahoo Japan
  - *.yahoo-net.jp
- Yahoo Mail
  - mail.yahoo.com/cal/ (this is the same as calendar.yahoo.com and should be reported as Yahoo Calendar)
- Yahoo Messenger
  - Yahoo Messenger Android
  - Yahoo Messenger iOS
  - Yahoo Messanger (web)

    - Store Editor
    - YSB Developer Network
    - Commerce Central
    - Localworks
    - Luminate
    - Wizards
    - **All other YSB related products/services/sites**
    - https://s.yimg.com/pq/*
    - *.webhosting.yahoo.com

- Yahoo Sports: Editorial
    - shop.yahoosports.com (Third party)

- Yahoo Sports: Fantasy Games
    - *.sendbird.com (Third Party, SendBird)

- Yahoo Sports: Rivals
    - *.rivalsfanstore.com (3rd party, Fanatics Inc.)
    - *.rivalscamps.com (3rd party)
    - *.rivalscampseries.com (3rd party)
    - Rivals iOS

- *.yahoo.com.tw
- *.yahoo.net

Other

SSP Advertising Products

These products with their listed domains are NOT eligible for bounty or reputation for the time being:

- CRS - crs-prd.aws.oath.cloud
- Deals UI - deals.o2.verizonmedia.com
- O2 - adaptv.advertising.com
- OneAdServer - console.oneadserver.aol.com
- OneAPI - oneapi.aol.com
- OneCreative - onecreative.aol.com
- OneInsights - alephd.com
- OneMobile - onemobile.aol.com
- OneReporting - vidible.tv
- OneVideo - onevideo.aol.com
- SSP - ssp.verizonmedia.com
- SSP External API - ext.api.ssp.aol.com
- Store - store.vzbuilders.com, sales.oath.com

Note: Any domains for these products that is not listed here is ALSO not eligible for bounty or reputation.

Download Burp Suite Project Configuration file (16 URLs) View changes Last updated on October 12, 2021.

about 1 day

Average time to first response

3 days

Average time to triage

17 days

Average time to bounty

96% of reports

Meet response standards

Based on last 90 days

Program Statistics

Updated Daily

>$21,520,000

Total bounties paid

$500

Average bounty

$6,500 - $40,000

Top bounty range

$170,000

Bounties paid in the last 90 days

468

Reports received in the last 90 days

2 days ago

Last report resolved

10594

Reports resolved

Top hackers

mayonaise	Reputation:14681
dawgyg	Reputation:14056
nnwakelam	Reputation:12656
todayisnew	Reputation:8786
meals	Reputation:7135

All Hackers

Directory
Leaderboard
Docs
Disclosure Guidelines
Privacy

Security
Blog
Support
Press
Terms

HackerOne